Energy firms must acknowledge cybersecurity as more than an IT problem, paper claims

September 21 2012, by Jeff Falk

(Phys.org)—Energy firms have spent vast sums on the security of their information systems, but they must reorient from a reactive, tactical posture regarding intrusions and attacks to a more strategic, holistic view that expands beyond the categorization of the issue as an IT problem, according to a new paper from Rice University's Baker Institute for Public Policy.

Titled "Cybersecurity Issues and Policy Options for the U.S. Energy Industry," the paper investigates how energy companies involved in the production and delivery of hydrocarbons, as well as companies that generate and transmit electricity, face new risks posed by malicious software ("malware"). These risks can affect the continuity of their operations, capacity to deliver products and services and ability to protect investments—particularly in research and development—from theft or unauthorized disclosure.

The paper comes against the backdrop of the U.S. Congress' failure this summer to pass significant cybersecurity legislation for the protection of commercial and government information technology infrastructure.

"For the energy industry, cybersecurity is not just a technology problem, but rather is one that includes the larger dynamics of information and operations," said Christopher Bronk, the paper's principal author and a Baker Institute fellow in information technology policy. "How public

policy can form components of the response to cybersecurity issues pertaining to the energy industry and the critical infrastructure that it builds, operates and maintains requires considering both the complexity of the issue and the nuance in potential policy prescriptions."

The paper details examples of major oil and gas companies that have suffered a significant data breach or disruption of IT service, the latest being Saudi Aramco. In August, Saudi Aramco saw as many as 30,000 computers on the company's network compromised by a malicious piece of "malware," possibly the one labeled "Shamoon" by the computer malware analysis community.

"The issues of cyberespionage and true cyberattacks—the ability to achieve kinetic outcomes by manipulation of computer systems—represent significant challenges for the energy industry, the United States government and the international community," Bronk said.

"Constructing institutions to cope with these problems and move beyond a reactive posture will require greater research investment, collaboration and unorthodox combinations of expertise from within the computing field and beyond it."

Provided by Rice University

Citation: Energy firms must acknowledge cybersecurity as more than an IT problem, paper claims (2012, September 21) retrieved 24 April 2024 from https://phys.org/news/2012-09-energy-firms-acknowledge-cybersecurity-problem.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.